KOREAN PATENT PUBLICATION (B1)

Patent No. : 10-0228021
Patent Date : August 6, 1999
Application No. : 10-1996-0075479
Application Date : December 28, 1996
Laid-Open Publication No. : 1998-0056214
Laid-Open Publication Date: September 25, 1998
Pantentee : SK TELECOM Co., Ltd., Seoul, Republic of Korea
Inventors : Hyun-Chang CHO, Pusan, Republic of Korea
Yong-Wook CHOI, Daejun, Republic of Korea
Jae-Wan PYUN, Daejun, Republic of Korea
Kyun-Suk CHUNG, Daejun, Republic of Korea

MOBILE COMMUNICATION TERMINAL HAVING SMART CARD AND METHOD FOR AUTHENTICATING SUBSCRIBER AND UPDATING SHARED SECRET DATA USING THE SAME

ABSTRACT

1. Field of the invention

The present invention relates to an authentication technique for excluding the illegal telephone call by the illegal reproduction of the mobile communication terminal.

2. Technical object of the invention

The present invention is to provide a mobile communication terminal having a smart card and a method for authenticating a subscriber and updating shared secret data using the same.

3. The present invention provides a mobile communication terminal having a smart card and a method for authenticating a subscriber and updating shared secret data using the same which can exclude an illegal telephone call by an illegal reproduction terminal by applying the advantage of the smart card and at the same time, provide new services, for example, a roaming, pre-paid service and banking service among different systems easily.

4. Usage of the invention

The present invention is used to authenticate a mobile communication terminal.

(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51)oInt. Cl.[6]
H04B 7/12

(11) 등록번호 10-0228021
(24) 등록일자 1999년08월06일

(21) 출원번호 10-1996-0075479
(22) 출원일자 1996년12월28일
(65) 공개번호 특1998-0056214
(43) 공개일자 1998년09월25일

(73) 특허권자 에스케이텔레콤주식회사 서정욱
서울특별시 중구 남대문로5가 267

(72) 발명자 조현창
대전광역시 유성구 전민동 삼성푸른아파트 112-1202
최용욱
대전광역시 유성구 전민동 삼성푸른아파트 112-1401
변재완
대전광역시 유성구 전민동 엑스포아파트 301-404
정규석
대전광역시 유성구 전민동 엑스포아파트 212-901

(74) 대리인 박해천, 원석희

심사관 : 임영희

(54) 스마트 카드를 구비한 이동통신 단말기 및 그를 이용한 가입자 인증방법과 공유 비밀데이터 갱신방법

요약

1. 청구범위에 기재된 발명이 속한 기술분야

본 발명은 이동통신 단말기의 불법복제에 의한 불법통화를 배제시키기 위한 인증기술에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

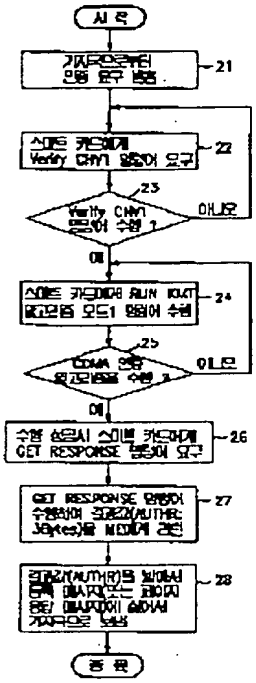
본 발명은 스마트 카드를 구비한 이동통신 단말기 및 그를 이용한 가입자 인증방법을 제공하고자 함.

3. 발명은 스마트 카드의 장점을 충분히 살려 이동전화 시스템에 적용하므로써, 불법복제 단말기에 의한 불법통화를 원천적으로 배제시키는 동시에, 새로운 부가 서비스들, 예컨대 서로 다른 시스템간의 로밍, 선불(Pre-paid)서비스, 뱅킹(Banking)서비스 등을 용이하게 제공할 수 있도록 하는 스마트 카드를 구비한 이동통신 단말기 및 그를 이용한 가입자 인증방법을 제공한다.

4. 발명의 중요한 용도 ....

이동통신 단말기의 인증에 이용됨.

대표도



명세서

도면의 간단한 설명

제1도는 본 발명에 따른 이동통신 단말기에 구비되는 스마트 카드의 내부 파일구조를 나타낸 일실시예 개략도.

제2도는 본 발명에 따른 이동통신 단말기에서의 인증자를 이용한 가입자인증 수행절차를 나타낸 일실시예 개략도.

제3(a)도는 상기 제2도에 따른 위치등록(Registration) 및 착호(Termination)인증과정에서 COMA 인증 알고리즘 수행시에 사용되는 입력 및 출력 데이터 포맷.

제3(b)도는 상기 제2도에 따른 발호(Origination)인증과정에서 COMA인증 알고리즘 수행시에 사용되는 입력 및 출력 데이터 포맷.

제3(c)도는 상기 제2도에 따른 단일시도(Unique Challenge)인증과정에서 COMA인증 알고리즘 수행시 사용되는 입력 및 출력 데이터 포맷.

제4도는 본 발명에 따른 이동통신 단말기에서의 공유비밀데이터(SSD)갱신 메시지 처리절차를 나타낸 일실시예 개략도.

제5(a)도는 본 발명에 따른 이동통신 단말기에서의 카운트(COUNT)값 요구에 대한 수행절차를 나타낸 일실시예 개략도.

제5(b)도는 본 발명에 따른 이동통신 단말기에서의 카운트값 갱신요구에 대한 수행절차를 나타낸 일실시예 개략도.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 이동통신 단말기의 불법복제에 의한 불법통화를 배제시키기 위한 인증기술에 관한 것으로, 특히 스마트 카드를 구비한 이동통신 단말기 및 그를 이용한 가입자 인증방법과 공유비밀데이터 갱신방법에 관한 것이다.

종래의 이동통신 시스템의 경우, 예컨대 셀룰라 이동전화기의 경우, 불법복제 단말기에 의한 불법통화의 문제점이 심각하게 대두되고 있다. 이는 근본적으로 단말기의 모든 데이터는 복제가 가능하기 때문에 발생하는 것으로, 단말기에 의한 인증의 한계를 드러내고 있는 것이다.

마찬가지로, CDMA(Code Division Multiple Access) 디지털 시스템의 경우도 최근에 상용 서비스를 시작하였으나, 기존 AMPS(Advanced Mobile Phone System)에서 일어나는 불법복제 단말기에 의한 불법통화의 문제점은 여전히 상존하고 있다.

또한, 통신분야의 세계적인 추세는 점점 단일 서비스권화되어 가고 있지만, CDMA방식을 취하는 우리나라의 이동전화 시스템과 세계의 다른 여러나라 시스템간의 로밍서비스는, 상호간의 시스템이 서로 다르기 때문에 현재의 단말기를 통해서는 구현 불가능하다는 기술적인 한계가 있다.

발명이 이루고자하는 기술적 과제

본 발명은 상기한 바와 같은 종래의 제반 문제점들을 해결하기 위해 안출된 것으로서, 스마트 카드의 장점을 충분히 살려 이동전화 시스템에 도입하므로써, 불법복제 단말기에 의한 불법통화를 원천적으로 배제시키는 동시에, 새로운 부가 서비스들(예컨대, 서로 다른 시스템간의 로밍, 선불(Pre-paid)서비스, 뱅킹(Banking)서비스 등)을 용이하게 제공할 수 있도록 하는 스마트 카드를 구비한 이동통신 단말기 및 그를 이용한 가입자 인증방법과 공유비밀데이터 갱신방법을 제공하는데 그 목적을 두고 있다.

이를 위해, 본 발명에서는 기존의 CDMA셀룰라폰 등의 이동통신 단말기에 스마트 카드를 부가하되, 그 스마트 카드에 가입자 인증 알고리즘과, CDMA 등의 인증에 관련된 명령어와, CDMA 등의 이동통신에 관한 파라미터를 정의하여 구비시킬 뿐만 아니라, 상기한 바와 같은 스마트 카드를 구비한 이동통신 단말기에서 인증자 또는 카운트 값을 비교하여 가입자에 대한 인증을 수행하는 방법과 공유비밀데이터 갱신방법을 제시한다.

발명의 구성 및 작용

본 발명은 상기 목적을 달성하기 위하여, 공지의 이동통신 단말기에 스마트 카드를 구비시키되, 상기 단말기의 파라미터들 중 가입자에 관한 정보 및 인증에 관련된 정보는 상기 스마트 카드에 저장하고, 단말기에 관한 정보는 상기 공지의 단말기에 분리하여 저장한 것을 특징으로 하는 스마트 카드를 구비한 이동통신 단말기를 제공한다.

그리고, 상기 스마트 카드의 내부 파일 구조는, 전체 디렉토리에 해당하는 하나의 마스터 파일(MF; Master File)과, 서브 디렉토리에 해당하는 적어도 하나의 전용파일(DF; Dedicated File), 및 필요한 내용을 저장하는 다수의 단위 파일(EF; Elementary File)을 포함하고 있으며, 상기 각 파일을 식별하기 위한 파일 식별자(ID; Identification)가 할당되고, 파일 지정시 상기 파일 식별자(ID)를 이용하여 이루어지는 것을 특징으로 한다.

또한, 본 발명은 상기 목적을 달성하기 위하여, 이동통신 단말기에 스마트 카드가 구비되되, 상기 단말기의 파라미터들 중 가입자에 관한 정보 및 인증에 관련된 정보는 상기 스마트 카드에 저장되고, 상기 단말기에 관한 정보는 상기 단말기에 분리하여 저장된 이동통신 단말기를 이용한 가입자 인증방법에 있어서, 기지국으로부터 인증을 요구받아 상기 스마트 카드 내부에 있는 CHV(Card Holder Verification)값을 확인하는 명령어(Verify CHV1)의 실행을 요구하는 제1단계; 상기 스마트 카드 내부에 있는 CHV(Card Holder Verification)값을 확인하는 제2단계; 상기 제2단계의 실행이 완료되면 상기 스마트 카드에 특정 인증알고리즘(RUN ALGORITHM)명령어의 실행을 요구하는 제3단계; 상기 스마트 카드에서 인증알고리즘을 수행하는 제4단계; 바로 전의 명령어에 의해서 상기 스마트 카드 내부에 생성된 결과값을 가져오는 명령어(RESPONSE)의 실행을 상기 스마트 카드에 요구하는 제5단계; 상기 스마트 카드에서 상기 바로 전의 명령어에 의해서 스마트 카드 내부에 생성된 결과값을 가져오는 명령어(GET RESPONSE)를 실행하여 인증결과 값(AUTHR)을 출력하는 제6단계; 및 상기 단말기에서 그 인증결과값(AUTHR)을 입력받아 기지국으로 출력하는 제7단계를 포함하는 것을 특징으로 한다.

그리고, 상기 제4단계에서 수행되는 해당 인증알고리즘은 위치등록(Registrtion)인증, 착호(Termination)인증, 발호(Origination)인증 또는 단일시도(Unique Challenge)인증 중 어느 하나인 것을 특징으로 한다.

또한, 이동통신 단말기에 스마트 카드가 구비되되, 상기 단말기의 파라미터들 중 가입자에 관한 정보 및 인증에 관련된 정보는 상기 스마트 카드에 저장되고, 상기 단말기에 관한 정보는 상기 단말기에 분리하여 저장된 이동통신 단말기에서의 공유 비밀 데이터(SSD) 갱신 방법에 있어서, 기지국으로부터 공유 비밀 데이터(SSD) 갱신요구메세지를 통해 랜덤값(RAND SSD)을 받아 상기 단말기에 저장하는 제1단계; 상기 스마트 카드에 결과값도출(ASK RANDBS)명령어 실행을 요구하여, 상기 스마트 카드에서 실행된 결과값(RANDBS)이 스마트 카드에 저장되도록 함과 동시에 그 결과값을 상기 단말기에 받는 제2단계; 상기 단말기가 결과값(RANDBS)을 다시 기지국으로 보내고 나서, 스마트 카드로 공유 비밀 데이터갱신(Update SSD)명령어의 실행을 요구하는 제3단계; 상기 스마트 카드가 공유 비밀 데이터 생성 알고리즘(SSD Creation Algorithm)을 수행하여 새로운 공유 비밀 데이터(SSD_A, SSD_B)를 생성하는 제4단계; 상기 단말기가 기지국으로부터 기지국 시도 확인(Base Station Challenge Confirmation)메세지를 받아 상기 스마트 카드에 공유 비밀 데이터 확인(Confirm SSD)명령어의 실행을 요구하는 제5단계; 상기 스마트 카드가 인증 알고리즘을 수행하여 결과값(AUTHBS')을 생성하고 나서, 기지국으로부터 받은 인증센타의 결과값(AUTHBS)과 상기 CDMA인증알고리즘을 수행하여 얻은 결과값(AUTHBS')을 비교하는 제6단계; 및 상기 제6단계의 비교결과가 일치하는 경우에, 현재의 공유 비밀 데이터(SSD_A, SSD_B)값이 상기 새로이 생성된 공유 비밀 데이터(SSD_A 및 SSD_B)로 갱신되며, 그 사실이 상기 단말기에 통보되어, 상기 단말기가 기지국에게 통보하는 제7단계를 포함하는 것을 특징으로 한다.

한편, 이동통신 단말기에 스마트 카드가 구비되되, 상기 단말기의 파라미터들 중 가입자에 관한 정보 및 인증에 관련된 정보는 상기 스마트 카드에 저장되고, 상기 단말기에 관한 정보는 상기 단말기에 분리하여 저장된 CDMA 이동통신 단말기를 이용한 가입자 인증방법에 있어서, 상기 스마트 카드로부터 CDMA 인증을 수행한 결과값(AUTHR)을 받는 제1단계; 상기 스마트 카드로 카운트 읽기(READ BINARY (COUNT))명령어 실행을 요구하는 제2단계; 상기 스마트 카드에서 카운트 읽기 실행이 완료되면 결과 카운트(COUNT)값을 받아서 기지국으로 보내어 상기 기지국에서 그 결과 카운트 값을 다시 인증센터로 보내도록 하는 제3단계; 상기 인증센터에서 상기 스마트 카드에서 읽어온 상기 결과 카운트(COUNT)값과 상기 인증센터가 가지고 있는 카운트(COUNT)값을 비교하는 제4단계; 및 상기 제4단계의 비교결과가 일치하는 경우에만, 그 전화번호에 대해서 전화통화를 허용하는 제5단계를 포함하는 것을 특징으로 한다.

이하, 첨부된 도면을 참조하여 본 발명의 일실시예를 상세히 설명하기로 한다.

제1도는 본 발명에 따른 이동통신 단말기에 구비되는 스마트 카드의 내부 파일 구조를 나타낸 일실시예 개략도로서, 현재 상용중인 CDMA 이동전화 시스템용의 스마트 카드를 그 일예로서 제시하는 것이다.

본 실시예에서는 스마트 카드 내부에, CDMA 인증에 관련된 명령어, 스마트 카드 내부에 저장해 둘 CDMA 이동통신에 관한 파라미터를 정의하여, CDMA용 스마트 카드를 구현한 것이다.

이와 같은 CDMA 셀룰라 이동통신을 위한 스마트 카드 설계에 관한 사항은, 크게 다음의 세가지 분야로 나누어 설명할 수 있다.

A. 물리적 특성, 전기 신호 및 전송프로토콜

본 실시예의 스마트 카드의 물리적 특성은 ISO-7816 파트1, 파트2, 및 파트3을 따른다. 그리고, 상기 스마트 카드의 전기 신호 및 전송프로토콜은 ISO-7816 파트와 GSM 11.11의 국제 표준을 따른다.

B. CDMA 인증 관련 명령어 및 카운트(COUNT)처리 방법

기본적으로 스마트 카드가 도입됨으로써 기존의 단말기 내부 처리 부분 중 인증에 관련된 중요한 과정 즉, 인증 알고리즘을 수행하는 부분 등은 모두 스마트 카드에서 이루어지도록 하고, 단말기(Mobile Equipment: ME)는 단지 통신에 관련된 무선(RF)처리만 담당하는 것으로 한다.

스마트 카드와 단말기(ME)간의 인터페이스를 위해서는 미리 약속되어진 스마트 카드용 명령어가 필요하다.

기존의 이동통신용 카드 명령어는 GSM 11.11에 잘 정의되어 있으며, CDMA 인증과정은 IS-95에 단말기와 기지국 사이의 메시지가 정의되어 있지만, 상기 단말기(ME)와 스마트 카드 사이의 메시지는 정의되어 있지 않다. 따라서, 본 실시예에서는 CDMA 인증에 관련된 명령어를 먼저 정의하고, 각 인증 과정에 대해 스마트 카드와 단말기(ME)사이에 메시지 처리 방법을 제시한다.

IS-95에서는 각각의 인증에 관련된 입출력 파라미터를 정의하고 있는데, 본 실시예에서는 기존의 단말기에 스마트 카드를 추가하고, 인증에 관련된 중요한 파라미터들은 상기 스마트 카드 내부 영역에 저장하여 불법복제로부터 보호한다.

그리고, 파라미터 중에는 단말기 고유번호(ESN)가 포함되는데, 이 파라미터가 인증과 관련하여 사용된다. 특히, 본 발명에서는 인증에 관련된 중요한 데이터는 스마트 카드 내부에 저장하는 것을 원칙으로 하기 때문에, 스마트 카드 내부에 스마트 카드 식별자(SC_ID)로 상기 단말기 고유번호(ESN)와 똑같은 값을 생성하여 처리하도록 한다.

각각의 인증에 관련하여 파라미터와 스마트 카드 명령어를 정리하면, 다음의 표1과 같다.

[표 1]

IS-95 한동자 생성 알고리즘의 입출력 파라미터와 스마트 카드 인증 명령어

동작 코드	외부 입력	내부 입력(스마트 카드 내부)			스마트카드 명령어
최초등록 /재등록	RAND(32)	SC_ID(32)	MIN1(24)	SSD_A(64)	RUN ALGORITHM mode 1
발호 인증	RAND(32) Digits(24)	SC_ID(32)		SSD_A(64)	RUN ALGORITHM mode 2
유일시도(Unique Challenge)	RANDU(24)	SC_ID(32)	MIN1(24) MIN2(8)	SSD_A(64)	RUN ALGORITHM mode 3
기지국 시도 (Base Station Challenge)		SC_ID(32)	MIN1(24) RANDBS(32)	New SSD_A(64)	ASK RANDBS, UPDATE SSD, CONFIRM SSD

상기 인증 알고리즘(RUN ALGORITHM)명령어는 불법적인 통신행위를 방지하기 위해서 스마트 카드의 적법성을 확인하기 위한 것이다.

위치등록, 이동국 발호, 이동국 착호, 유일시도인 경우 스마트 카드 내부에서 상기 인증알고리즘(RUN ALGORITHM)을 수행하고, 그 결과(AUTHR)를 계산하여 인증센타로 보내므로서, 인증센타에서 계산한 값과 비교하여 인증을 수행하는 것이다.

상기 랜덤값 생성요구(ASK RANDBS)명령어는 기지국 시도(Base Station Challenge)인증과정 중에 첫 번째 일어나는 것으로, 스마트 카드에 랜덤(RANDOM)값인 "RANDBS"(4바이트)의 생성을 요구하는 명령이다.

상기 공유 비밀데이터 생성(UPDATE SSD)명령어는 기지국 시도(Base Station Challenge)인증과정 중에 두 번째 일어나는 것으로 인증과 관련한 새로운 공유 비밀 데이터(New SSD_A, New SSD_B)의 값을 생성한다.

상기 공유 비밀데이터 확인(CONFIRM SSD)명령어는 기지국 시도(Base Station Challenge)인증과정 중에 스마트 카드 내부적으로 상기 랜덤값(RANDBS)을 가지고 인증알고리즘을 작동시켜서 인증결과(AUTHBS')를 생성한다. 그리고, 인증센터에서 계산한 결과(AUTHBS)와 상기 스마트 카드 내부에서 계산한 결과(AUTHBS')가 일치하는지 여부를 검사하여, 일치하면 기존의 공유 비밀 데이터(SSD_A, SSD_B)값을 상기 새로운 공유 비밀 데이터(New SSD_A, New SSD_B)의 값으로 바꾸는 일을 한다.

C. 스마트 카드 내부 파일 구조 및 내용

CDMA 단말기 내부의 파라미터들 중, 가입자에 관한 모든 정보(예를 들면, 가입자 전화번호(MIN)와 인증에 관련된 정보는 스마트 카드에 저장하고, 단말기에 관한 정보는 단말기(ME)에 그대로 저장한다.

본 실시예에 따른 스마트 카드의 내부 파일 구조를 제1도를 참조하여 살펴보면, 먼저 전체 디렉토리에 해당하는 마스터 파일(MF; Master File)(11)과, 서브 디렉토리에 해당하는 전용 파일(DF; Dedicated File)(12, 13)과, 필요한 내용을 저장하는 다수의 단위 파일(EF; Elementary File)(14, 15, 16)들을 포함하고 있다.

그리고, 상기 각 파일을 식별하기 위한 파일 식별자(ID; Identification)가 사용되는데, 본 실시예에서는 2바이트로 구성하였으며, 다음과 같이 그 첫 번째 바이트로 상기 마스터 파일(MF)(11)과, 전용 파일(DF)(12, 13)과, 단위 파일(EF)(14, 15, 16)들을 구별하고 있다.

-'3F': 마스터 파일(MF)

-'7F': 전용 파일(DF)

-2'F': 마스터 파일(MF)밑에 속해있는 단위 파일(EF).

-6'F': 전용 파일(DF)밑에 속해있는 단위 파일(EF).

그리고, 상기 단위 파일(EF) 식별자(ID)들은 같은 전용 파일(DF)밑에 속해 있는 경우에는 똑같은 식별자(ID)를 사용할 수 없지만, 다른 전용 파일(DF) 밑에 속해 있는 경우에는 같은 식별자(ID)를 사용하여도 무방하다. 또한 각 파일은 선택(Select)명령으로 이루어지며, 모든 파일 지정은 파일 식별자(ID)를 사용하여 이루어진다.

CDMA 스마트 카드의 전용 파일(DF)은 기본적인 통신서비스를 담고 있는 부분(일명 "텔리콤(Telecom)"이라 칭함)과, CDMA 통신 서비스와 관련된 파라미터를 담고 있는 부분(일명 "CDMA"라 칭함)은 기본적으로 들어가야 한다. 그리고 CDMA 통신에 관해서 스마트 카드에 담아야 하는 기본 파라미터를 정리하여 각각 하나의 단위 파일(EF)로 만들어야 한다.

앞에서 예시한 제1도의 전체 파일 내용은 다음의 표 2와 같다.

또한, CDMA 시스템에서 가입자 인증은 인증자를 이용한 인증과, 카운트(COUNT)값을 비교하는 인증으로 나눌 수 있다.

먼저, 인증자를 이용한 인증은 크게 4가지로 나눌 수 있는 바, IS-95를 참고로하여 정리하면, 등록(Registration)인증, 유일시도(Unique Challenge)인증, 발호(Origination)인증 및 착호(Termination)인증으로 나눌 수 있다.

[표 2]

파일명	내 용
IC_ID	-CDMA 스마트 카드의 고유한 숫자
LP	-선호된 언어(Language Preference)
MIN1	-가입자 전화번호 1 (Mobile Station Identification Number 1)
MIN2	-가입자 전화번호 2 (Mobile Station Identification Number 2)
SSD_A	-공유 비밀데이타(Shared Secret Data) -인증과 관련하여 사용되는 데이터
SSD_B	-공유 비밀데이타(Shared Secret Data) -인증과 관련하여 사용되는 데이터
COUNT	-인증과 호별 사용방지를 사용 -0 부터의 수로 시스템과 스마트(SIM) 카드가 동시에 관리
SMSPS	-시스템 식별자, 네트워크 식별자, 첫번째 채널, 두번째 채널 (SID NID Primary channel Secondary channel • 시스템 식별자(SID): 서로다른 시스템을 식별하는 숫자 • 네트워크 식별자(NID): 네트워크 식별자(Network Identification)로 같은다 시스템 안에 네트워크를 세분하는 숫자 • 첫번째 채널(Primary channel): 단말기가 처음 시스템을 억속하는데 사용되는 주파수 채널 • 두번째 채널(Second channel): 단말기가 처음 시스템을 억속한 때 첫번째 채널이 할당되지 않을 때 사용되는 주파수 채널
ACC	-접근 과부하 등급(Access Overload Class) -특별사항이나 시스템이 과부하되었을때 단말기가 시스템에 접근시 제한을 가하는 변수
FSID	-금지된 시스템 식별자들(Forbidden SIDs)
PHASE	-스마트 카드의 버전(Phase version)
AS	-현재 사용 가능한 시스템(Acquisition SID)
HSR	-등록이 되면 단말기 작신(terminated call) 가능함(Home System Registration)
FSR	-등록이 되면 타시스템에 있어도 자동 등록이 가능함(Foreign SID Registration)
FNR	-등록이 되면 단말기가 외부 네트워크에 있을 때 작신(terminated call) 가능함(Foreign NID Registration)
FFPC	-우선수 A채드와 B채드의 페이징 채널 번호(FW First Paging Channel)
FHSY	-아나로그 자기 시스템 번호(FW Home SID number)
FAS	-아날로그(FM) 서비스가 가능한 시스템 번호(FM Acquisition SID)
FLS	-아날로그 서비스가 잠겨진 시스템 번호(FW Lock SID)
FAR	-자동등록이 가능한지 여부를 결정(FW Auto Registration)
CAI	-선불(Pre-paid) 카드 서비스와 관련하여 분 단위당 시간 가격 규모 변수(scale factor)의 정보를 담은 파일(Charge Advice Information)
ACM	-선불(Pre-paid) 카드 서비스와 관련하여 현재까지 통화된 호(call) 등의 합 (Accumulated call meter)
ACMmax	-ACM의 최대값(Accumulated call meter Maximum value)
A_KEY	-인증에 관련된 키 값

제2도는 본 발명에 따른 CDMA 이동통신 단말기에서의 인증자를 이용한 가입자 인증 수행절차를 나타낸 일실시예 개략도이고, 제3(a)도는 상기 제2도에 따른 위치 등록(Registrtion) 및 착호(Termination) 인증과정에서 CDMA 인증 알고리즘 수행시에 사용되는 입력 및 출력 데이터 포맷도이고, 제3(b)도는 상기 제2도에 따른 발호(Origination)인증과정에서 CDMA 인증 알고리즘 수행시에 사용되는 입력 및 출력 데이터 포맷도이며, 제3(c)도는 상기 제2도에 따른 단일시도(Unique Challenge) 인증과정에서 CDMA 인증 알고리즘 수행시 사용되는 입력 및 출력 데이터 포맷도이다.

제2도에 도시된 바와 같이, 본 발명에 따른 CDMA 이동통신 단말기에서의 인증자를 이용한 가입자인증 수행절차는, 기지국으로부터 인증을 요구받아 상기 스마트 카드 내부에 있는 CHV(Card Holder Verfication)값을 확인하는 명령어(Verify

CHV1)의 실행을 요구하면(21, 22), 그에 따라 상기 스마트 카드 내부에 있는 CHV(Card Holder Verfication)값을 확인하고(23), 그 실행이 완료되면 상기 스마트 카드에 특정 인증알고리즘(RUN ALGORITHM)명령어의 실행을 요구하여(24), 상기 스마트 카드에서 해당 인증알고리즘이 수행되도록 한 후(25), 바로전의 명령어에 의해서 스마트 카드 내부에 생성된 결과값을 가져오는 명령어(GET RESPONSE)를 실행하여 인증결과값(AUTHR)을 출력하도록 하고(27), 단말기에서 그 인증결과값(AUTHR)을 입력받아 기지국으로 출력하는 것(28)에 의해 이루어짐을 알 수 있다. 이때, 상기 해당 인증알고리즘은 위치 등록(Registrtion)인증, 착호(Termination)인증, 발호(Origination)인증 또는 단일시도(Unique Challenge)인증 중 어느 하나를 수행한다.

그리고, 상기 위치 등록(Registrtion) 및 착신(Termination) 인증 알고리즘 수행시 이용되는 입력데이터는, 외부 파라미터인 난수값(RAND)과, 스마트 카드 내부 파라미터인 스마트카드 고유식별자(SC_ID), 가입자 전화번호(MIN1), 및 인증관련 데이터인 공유 비밀 데이터(SSD_A)로 구성되고, 상기 발신(Origination)인증 알고리즘 수행시 이용되는 입력 데이터는, 외부 파라미터인 난수값(RAND)과, 스마트 카드 내부 파라미터인 스마트 카드 고유식별자(SC_ID)와, 외부 파라미터인 발신번호(DIGITS) 내부 파라미터인 공유 비밀 데이터(SSD_A)로 이루어지며, 상기 단일시도(Unique Challenge) 인증 알고리즘 수행시 이용되는 입력 데이터는, 외부 파라미터인 난수값(RAND)과, 스마트카드 내부 파라미터인 제1 및 제2가입자 전화번호(MIN1, MIN2), 스마트카드 고유식별자(SC_ID) 및 인증 관련 데이터인 공유비밀 데이터(SSD_A)로 이루어진다.

제4도는 본 발명에 따른 이동통신 단말기에서의 공유 비밀 데이터(SSD) 갱신 절차를 나타낸 일실시예 개략도이다.

도면에 도시된 바와 같이, 본 발명에 따른 CDMA 이동통신 단말기에서의 공유 비밀 데이터(SSD)값 갱신 수행절차는, 기지국으로부터 공유 비밀 데이터(SSD) 갱신요구메세지를 통해 랜덤값(RAND SSD(56bits))을 받아 단말기에 저장하고(41), 스마트카드에 결과값도출(ASK RANDBS)명령어의 실행을 요구하여(42), 상기 스마트카드에서 실행된 결과값(RANDBS)을 스마트카드에 저장함과 동시에 그 결과값을 단말기로 보낸다(43).

단말기는 그 결과값(RANDBS)을 다시 기지국 시도 요구 메시지(Base Station Challenge Order Message)에 실어서 기지국으로 보내고(44)나서, 스마트 카드로 공유 비밀 데이터갱신(Update SSD)명령어의 실행을 요구한다(45).

그러면, 스마트 카드가 공유 비밀 데이터 생성 알고리즘(SSD Creation Algorithm)을 수행하여 새로운 공유 비밀 데이터(SSD_A, SSD_B)를 생성한다(46), 그리고 나서, 단말기가 다시 기지국으로부터 기지국 시도 확인(Base Station Challenge Confirmation)메세지를 받아 스마트 카드에 공유 비밀 데이터 확인(Confirm SSD)명령어의 실행을 요구한다(47).

그러면, 스마트 카드가 CDMA 인증알고리즘을 수행하여 결과값(AUTHBS')을 생성하고(48)나서, 기지국으로부터 받은 인증센터의 결과값(AUTHBS)과 상기 CDMA 인증알고리즘을 수행하여 얻은 결과값(AUTHBS')을 비교하여(49), 일치하면 현재의 공유 비밀 데이터(SSD_A, SSD_B)값을 상기 새로이 생성된 공유 비밀 데이터(SSD_A 및 SSD_B)로 갱신하고(51), 그 사실을 단말기로 통보하여, 상기 단말기가 공유 비밀 데이터 갱신 확인 요구(SSD Update Confirmation Order) 메시지를 통해 기지국에게 보내지도록 한다(52).

반면에, 상기 인증센터의 결과값(AUTHBS)과 상기 CDMA 인증알고리즘을 수행하여 얻은 결과값(AUTHBS')을 비교한 결과가 다르면(49), 현재의 공유 비밀 데이터(SSD_A, SSD_B)값을 갱신하지 않고 그대로 둔 채로, 그 사실을 단말기로 통보하여, 상기 단말기가 공유 비밀 데이터 갱신 거절 요구(SSD Update Rejecion Oeder)메세지를 통해 기지국으로 보내도록 하는 것이다(50).

한편, CDMA 가입자 인증의 다른 하나의 방법으로서, 스마트 카드와 인증센타에서 지정하고 있는 카운트(COUNT)값을 비교하는 방법을 예로서 들 수 있다. 이때, 카운트 값을 비교하는 절차는 크게 카운트 요구 과정과 카운트 갱신 과정으로 구분할 수 있다.

제5(a)도는 본 발명에 따른 이동통신 단말기에서의 카운트(COUNT)값 요구에 대한 수행절차를 나타낸 일실시예 개략도이고, 제5(b)도는 본 발명에 따른 이동통신 단말기에서의 카운트 값 갱신요구에 대한 수행절차를 나타낸 일실시예 개략도이다

상기 카운트 요구 과정(제5(a)도)은 인증 수행시 또는 인증자를 받은 후, 수행된다. 그리고, 상기 카운트 갱신과정(제5(b)도)은 시스템에서 카운트 갱신 요구가 있을 경우 수행되는 것이며, 이러한 카운트 요구 과정과 카운트 갱신 과정은 새로운 명령어를 정의하지 않고, 기존의 유럽통신방식(GSM)명령어를 가지고 충분히 나타낼 수 있다.

우선, CDMA 이동통신 단말기에서의 카운트 요구 과정 수행 절차는, 제5(a)도에 도시된 바와 같이, 스마트 카드로부터 CDMA 인증을 수행한 결과값(AUTHR)을 받고 나서(511), 스마트 카드로 카운트 읽기(READ BINARY (COUNT))명령어 실행을 요구하며(512), 상기 스마트 카드에서 실행이 완료되면(513) 결과 카운트(COUNT)을 받아서 등록/발호 페이지 응답 메시지(Registration/Origination PageResponse Message)를 통해 기지국으로 보내며(514), 상기 기지국에서 그 결과 카운트(COUNT)값을 받아서 다시 인증센타로 보낸다(515).

그러면, 인증센타에서는 상기 스마트 카드에서 읽어온 상기 결과 카운트(COUNT)값과 인증센타가 가지고 있는 카운트(COUNT)값을 비교하여(516), 일치하면 그 전화번호에 대해서 전화통화를 허용하고(517), 반면에 상기 스마트 카드에서 읽어온 상기 결과 카운트(COUNT)값과 인증센타가 가지고 있는 카운트(COUNT)값이 서로 다르면 그 전화번호에 대해서는 전화통화를 정지시키는 것이다(518).

본 발명에 따른 CDMA 이동통신 단말기에서의 카운트 갱신 요구 과정 수행 절차는, 제5(b)도에 도시된 바와 같이, 단말기가 기지국으로부터 카운트 갱신 명령을 받으면(521), 스마트 카드에 카운트 읽기(READ BINARY(COUNT))명령어 실행을 요구하며(522), 상기 스마트 카드에서 카운트 읽기(READ BINARY)가 실행되도록 하며(523), 단말기에서 그 결과 카운트(COUNT)값을 받아서 +1한 후 다시 스마트 카드로 카운트 갱신(UPDATE BINARY(COUNT))명령어 실행을 요구한다(524). 그리고 나서, 상기 스마트 카드로부터의 결과 카운트(COUNT)값을 받아서 기지국으로 보내면(526), 상기 기지국은 그 결과 카운트 값을 받아서 다시 인증센터로 보내며(527), 상기 인증센터에서는 그 전화번호에 해당하는 카운트값을 1증가시키는 것이다(528).

발명의 효과

전술한 바와 같이 본 발명에 따르면, 기존의 CDMA 셀룰라폰 등의 이동전화 단말기에 스마트 카드를 부가하고, 그 스마트 카드에 가입자 인증 알고리즘과, CDMA 등의 인증에 관련된 명령어와, CDMA 등의 이동통신에 관한 파라미터를 정의하며, 그를 이용한 독특한 인증방법이 가능하도록 하므로써, 불법복제를 원천적으로 배제하도록 하였으며, 서로 다른 시스템간의 로밍문제와 다양한 응용서비스의 제공이 용이하도록 하는 효과를 갖는다.

(57) 청구의 범위

청구항 1. 공지의 이동통신 단말기에 스마트 카드를 구비시키되, 상기 이동 단말기의 파라미터들 중 가입자에 관한 정보 및 인증에 관련된 정보는 상기 스마트 카드에 저장되고, 단말기에 관한 정보는 상기 공지의 이동 단말기 내부에 각각 분리하여 저장되며, 상기 스마트 카드의 내부 파일 구조는, 전체 디렉토리에 해당하는 하나의 마스터 파일(MF)과, 서브 디렉토리에 해당하는 적어도 하나의 전용 파일(DF) 및 필요한 내용을 저장하는 다수의 단위 파일(EF)을 포함하되, 상기 각 파일들을 식별하기 위한 파일 식별자(ID)가 할당되어, 상기 각 파일들 중 특정 파일의 지정시 상기 파일 식별자(ID)를 이용하는 것을 특징으로 하는 스마트 카드를 구비한 이동통신 단말기.

청구항 2. 이동통신 단말기에 스마트 카드가 구비되되, 상기 단말기의 파라미터들 중 가입자에 관한 정보 및 인증에 관련된 정보는 상기 스마트 카드에 저장되고, 단말기에 관한 정보는 상기 단말기에 분리하여 저장된 이동통신 단말기를 이용한 가입자 인증방법에 있어서, 기지국으로부터 인증을 요구받아 상기 스마트 카드 내부에 있는 CHV(Card Holder Verification)값을 확인하는 명령어의 실행을 요구하는 제1단계; 상기 스마트 카드 내부에 있는 CHV값을 확인하는 제2단계; 상기 제2단계의 실행이 완료되면 상기 스마트 카드에 특정 인증알고리즘 명령어의 실행을 요구하는 제3단계; 상기 스마트 카드에서 인증 알고리즘을 수행하는 제4단계; 바로 전의 명령어에 의해서 상기 스마트 카드 내부에 생성된 결과값을

가져오는 명령어의 실행을 상기 스마트 카드에 요구하는 제5단계; 상기 스마트 카드에서 상기 바로 전의 명령어에 의해서 스마트 카드 내부에 생성된 결과값을 가져오는 명령어를 실행하여 인증결과 값(AUTHR)을 출력하는 제6단계; 및 상기 단말기에서 상기 인증결과값을 입력받아 기지국으로 출력하는 제7단계를 포함하는 것을 특징으로 하는 스마트 카드를 구비한 이동통신 단말기의 가입자 인증방법.

청구항 3. 제2항에 있어서, 상기 제4단계에서 수행되는 인증알고리즘은, 위치등록(Registrtion)인증, 착호(Termination)인증, 발호(Origination)인증, 또는 단일시도(Unique Challenge)인증 중 어느 하나인 것을 특징으로 하는 스마트 카드를 구비한 이동통신 단말기의 가입자 인증방법.

청구항 4. 제3항에 있어서, 상기 위치등록(Registrtion) 및 착호(Termination) 인증 알고리즘 수행시 이용되는 입력 데이터는 외부 파라미터인 난수값(RAND)과, 스마트카드 내부 파라미터인 스마트카드 고유식별자(SC_ID), 가입자 전화번호(MIN1), 및 인증관련 데이터인 공유 비밀 데이터(SSD_A)로 이루어진 것을 특징으로 하는 스마트 카드를 구비한 이동통신 단말기의 가입자 인증방법.

청구항 5. 제3항에 있어서, 상기 발호(Origination)인증 알고리즘 수행시 이용되는 입력 데이터는 외부 파라미터인 난수값(RAND)과, 스마트카드 내부 파라미터인 스마트카드 고유식별자(SC_ID)와, 외부 파라미터인 발신번호(DIGITS)와, 내부 파라미터인 공유 비밀 데이터(SSD_A)로 이루어진 것을 특징으로 하는 스마트 카드를 구비한 이동통신 단말기의 가입자 인증방법.

청구항 6. 제3항에 있어서, 상기 단일시도(Unique Challenge)인증 알고리즘 수행시 이용되는 입력데이터는 외부 파라미터인 난수값(RAND)과, 스마트카드 내부 파라미터인 제1 및 제2가입자 번호(MIN1, MIN2), 스마트카드 고유식별자(SC_ID) 및 인증관련 데이터인 공유 비밀 데이터(SSD_A)로 이루어진 것을 특징으로 하는 스마트 카드를 구비한 이동통신 단말기의 가입자 인증방법.

청구항 7. 이동통신 단말기에 스마트 카드가 구비되되, 상기 단말기의 파라미터들 중 가입자에 관한 정보 및 인증에 관련된 정보는 상기 스마트 카드에 저장되고, 단말기에 관한 정보는 상기 단말기에 분리하여 저장된 이동통신 단말기에서의 공유 비밀 데이터(SSD) 갱신 방법에 있어서, 기지국으로부터 공유 비밀 데이터(SSD) 갱신요구메세지를 통해 랜덤값(RAND SSD)을 받아 상기 단말기에 저장하는 제1단계; 상기 단말기에서 상기 스마트 카드로 결과값도출(ASK RANDBS)명령어 실행을 요구하여, 상기 스마트 카드에서 실행된 결과값(RANDBS)이 스마트 카드에 저장되도록 함과 동시에 그 결과값을 입력받는 제2단계; 상기 단말기가 상기 스마트 카드의 실행결과값(RANDBS)을 상기 기지국으로 전송한 후, 상기 스마트 카드로 공유 비밀 데이터갱신(Update SSD)명령어의 실행을 요구하는 제3단계; 상기 스마트 카드가 공유 비밀 데이터 생성 알고리즘을 수행하여 새로운 공유 비밀 데이터(SSD_A, SSD_B)를 생성하는 제4단계; 상기 단말기가 기지국으로부터 기지국 시도 확인 메세지를 받아 상기 스마트 카드에 공유 비밀 데이터 확인 명령어의 실행을 요구하는 제5단계; 상기 스마트 카드가 인증 알고리즘을 수행하여 결과값(AUTHBS')을 생성한 후, 상기 기지국으로부터 받은 인증센타의 결과값(AUTHBS)과 상기 스마트 카드의 결과값(AUTHBS')을 비교하는 제6단계; 및 상기 제6단계의 비교결과가 일치하는 경우에, 현재의 공유 비밀 데이터(SSD_A, SSD_B)값이 상기 새로이 생성된 공유 비밀 데이터(SSD_A 및 SSD_B)로 갱신되며, 그 사실을 상기 단말기를 통해 상기 기지국으로 통보하는 제7단계를 포함하는 것을 특징으로 하는 스마트 카드를 구비한 이동통신 단말기의 공유 비밀 데이터 갱신 방법.

청구항 8. 제7항에 있어서, 상기 제6단계의 비교결과가 다르면, 현재의 공유 비밀 데이터(SSD_A, SSD_B)값을 갱신하지 않고 그대로 둔 채, 그 사실이 상기 단말기로 통보되도록 하여, 상기 단말기가 공유 비밀 데이터 갱신 거절 요구 메시지를 통해 상기 기지국으로 통보하는 제8단계를 더 포함하는 것을 특징으로 하는 스마트 카드를 구비한 이동통신 단말기의 공유 비밀 데이터 갱신 방법.

청구항 9. 이동통신 단말기에 스마트 카드가 구비되되, 상기 단말기의 파라미터들 중 가입자에 관한 정보 및 인증에 관련된 정보는 상기 스마트 카드에 저장되고, 단말기에 관한 정보는 상기 단말기에 분리하여 저장된 CDMA 이동통신 단말

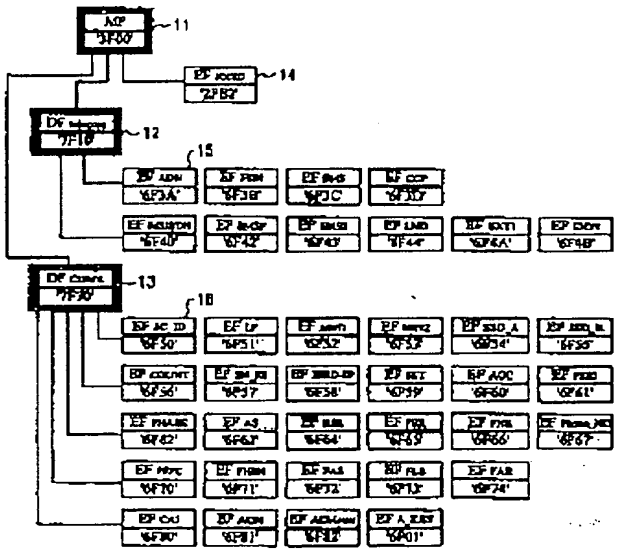
기를 이용한 가입자 인증방법에 있어서, 상기 스마트 카드로부터 COMA 인증을 수행한 결과값(AUTHR)을 받는 제1단계; 상기 스마트 카드로 카운트 읽기 명령어 실행을 요구하는 제2단계; 상기 스마트 카드에서 카운트 읽기 실행이 완료되면 그 결과 카운트 값을 받아서 상기 기지국을 통해 인증센터로 전송하는 제3단계; 상기 인증센터에서 상기 스마트 카드에서 읽어온 상기 결과 카운트(COUNT)값과 상기 인증센터가 가지고 있는 카운트(COUNT)값을 비교하는 제4단계; 및 상기 제4단계의 비교결과가 일치하는 경우에만, 그 전화번호에 대해서 전화통화를 허용하는 제5단계를 포함하는 것을 특징으로 하는 스마트 카드를 구비한 COMA 이동통신 단말기의 가입자 인증방법.

청구항 10. 제9항에 있어서, 카운트 갱신 요구가 있을 경우에 카운트 갱신을 수행하는 제6단계를 더 포함하는 것을 특징으로 하는 스마트 카드를 구비한 COMA 이동통신 단말기의 가입자 인증방법.

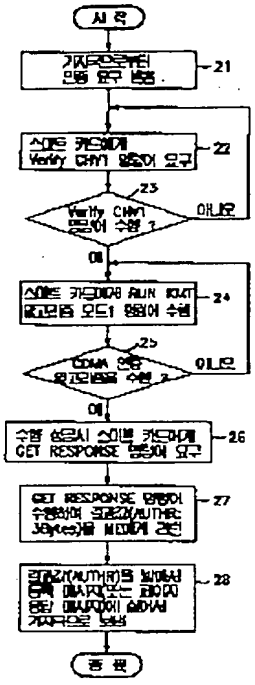
청구항 11. 제10항에 있어서, 상기 카운트 갱신을 수행하는 제6단계는, 상기 단말기가 상기 기지국으로부터 카운트 갱신 명령을 받으며, 상기 스마트 카드에 카운트 읽기 명령어 실행을 요구하는 제7단계; 상기 스마트 카드에서 카운트 읽기가 실행된 후, 상기 단말기에서 그 결과 카운트값을 받아서 임의의 제1값을 더한 후, 다시 상기 스마트 카드로 카운트 갱신 명령어 실행을 요구하는 제8단계; 상기 스마트 카드로부터의 결과 카운트 값을 받아서 상기 기지국을 통해 인증센타로 전송하는 제9단계; 및 상기 인증센터에서 그 전화번호에 해당하는 카운트 값을 상기 임의의 제1값만큼 증가시키는 제10단계를 포함하는 것을 특징으로 하는 스마트 카드를 구비한 이동통신 단말기의 가입자 인증방법.

도면

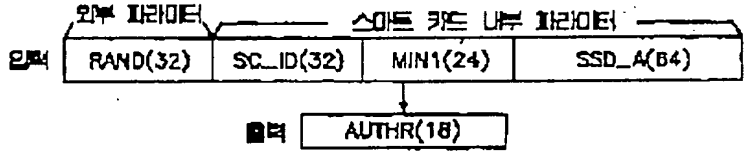
도면1



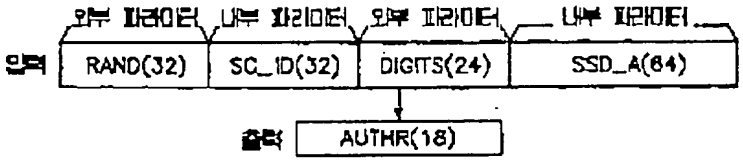
도면2


시작
21
22
23
아니오
예
24
25
아니오
예
26
27
28
종료

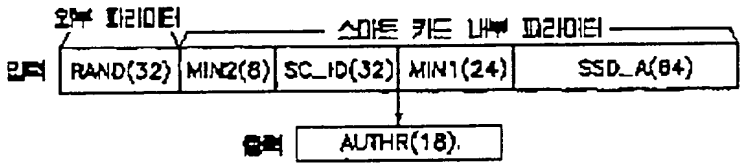
도면3a


외부 파라미터
스마트 카드 내부 파라미터
입력
RAND(32)
SC_ID(32)
MIN1(24)
SSD_A(64)
출력
AUTHR(18)

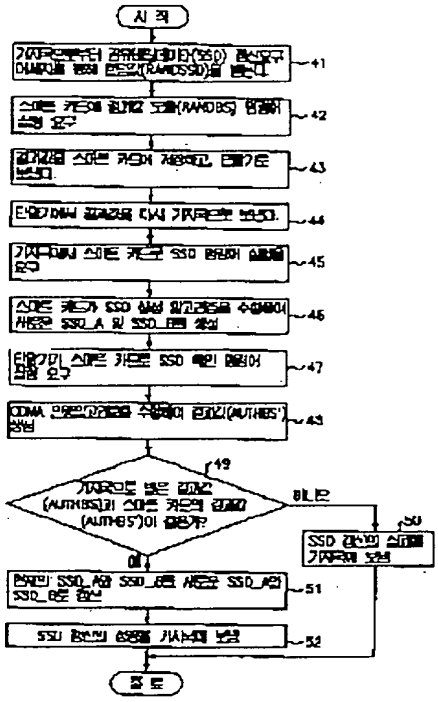
도면3b


외부 파라미터
내부 파라미터
외부 파라미터
내부 파라미터
입력
RAND(32)
SC_ID(32)
DIGITS(24)
SSD_A(64)
출력
AUTHR(18)

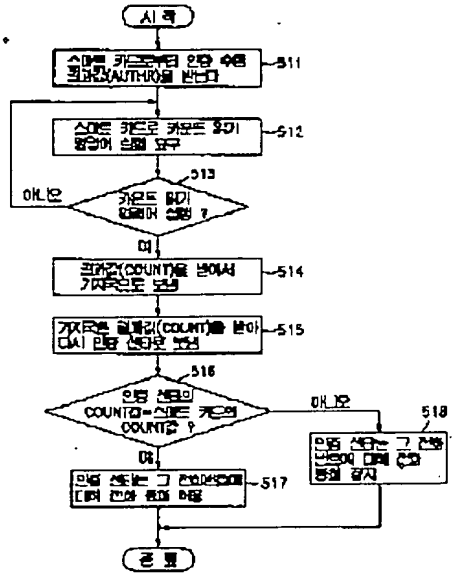
도면3a



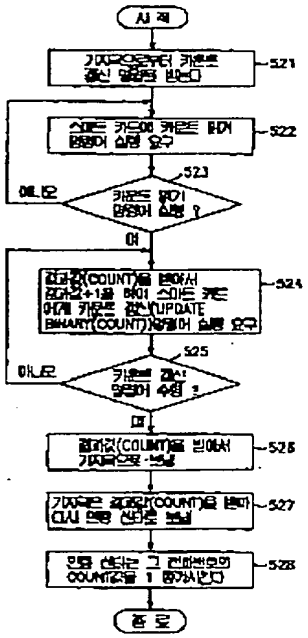
도면4



도면5a


시작
511
512
513
아니오
예
514
515
516
아니오
518
예
517
종료

도면5b


시작
521
522
523
아니오
예
524
525
아니오
예
526
527
528
종료